A conceptual information sharing framework to improve supply chain security collaboration

Authors' Version submitted to International Journal of Value Chain Management and Accepted on March 2nd, 2020

Ioannis Koliousis (ac8619@coventry.ac.uk) Coventry University, UK

Umair Tanveer (Umair.tanveer@bristol.ac.uk) University of Bristol, UK

Shamaila Ishaq (s.ishaq@derby.ac.uk) University of Derby, UK

Abstract

Modern Supply Chains are critical in terms of efficiency, economic activities and commercial impact, particularly in case of security incidents. Inland terminals, commercial ports and dry ports constitute key gateways for the transportation flows in these modern supply chains and are require enhanced security procedures. This paper develops a framework that facilitates the sharing of information among various supply chain stakeholders, which is expected to improve the security level from a value chain perspective. In this context, we propose the upgrade of the current security strategies utilizing existing processes, equipment in order to minimize time and cost currently needed but more importantly improving the level of security in the supply chain. A conceptual rule and role-based data fusion framework is developed enabling the seamless and timely exchange of messages. The proposed Data Fusion Framework has a simple architecture that supports quick integration to either network-based, distributed systems or conventional stand-alone systems and adheres to common data fusion principles. The proposed framework considers different components (e.g. sensors, algorithms and fusing procedures) in an equipment agnostic approach so as to enable easy access and easy usage of security information.

Keywords: Information systems, supply chain security; transport security; ICT; threat analysis; risk assessment; security awareness; data fusion; visibility; collaborative security

1 Introduction

1.1 Overview

It is a commonplace to suggest that the logistics sector is critical in terms of economic activities and commercial impact when security incidents occur. In this context, inland terminals, commercial ports and dry ports constitute key gateways for the transportation flows in these supply chains, and as such there is an increased need for enhanced security procedures, thus being a focal point in the Supply Chain Security. Therefore, these gateways have to rely not only on complicated and advanced facilities but also on advanced ICT infrastructure, on trustworthy e-supply chain services and robust procedures. The degradation, interruption or impairment of supply chain cargo flows have serious impacts on the economy, national security, health, safety, and the welfare of citizens and nations; thus the main objective of any decision maker is to either decrease the occurrence of these events or their impact.

This paper proposes a framework that focuses on improving the sharing of information among the supply chain stakeholders (agents). The proposed framework is expected to improve the security level of the entire supply chain. More precisely, the concept of this paper lies exactly on this premise, the more information becomes available to the decision maker, the more likely it is to minimize the probability of a Loss Event happening. Key success factor is the information availability, which should be based on specific sharing principles throughout the supply chain and to all relevant stakeholders. In this context upgraded security strategies may be developed upon existing processes minimizing time and cost currently needed but more importantly improving the level of security in the supply chain utilizing, even more, the existing security investment implemented by governmental bodies and private undertakings.

This paper is organized as follows: in the next section a literature review provides the broader context of the research. Section 2 presents the conceptual data fusion framework and its associated groups of architecture. Section 3 concludes with some important observations and section 4 provides some research and policy recommendations.

1.2 Literature Review

Before we describe the supply chain security in the cargo/container movement we would like to cover the supply chain in general and container supply chain in particular. A supply chain covers all activities associated with the flow and movement of goods, services, and related information from the point of origin to the point of consumption (Murphy and Wood, 2008). Currently, this flow and movement of goods, services and information are global in nature, transforming supply (value) chains into global supply (value) chains. Global supply chains are the international system of different entities/stakeholders including; suppliers, manufacturers, freight forwarders, logistics service providers, ocean carriers, buyers and custom authorities etc. that pave the way of international trade. Container shipping is an integral component of the transportation network that links the consigner and consignee and all other entities in the global supply chain responsible for the movement of material across the ocean.

Supply chain security has become a crucial element in the logistics operations and had gained the attention of researchers, especially after the disastrous events of September 11, 2001. According to Closs and McGarrell (2004) supply chain security management is "the application of policies, procedures, and technologies to protect supply chain assets (products, facilities, equipment, information, and personnel) from theft, damage, or terrorism, and to prevent the introduction of unauthorized contraband, people, or weapons of mass destruction into the supply chain". The security and the safety of the transportation networks are fundamental for the international trade (Closs and McGarrell, 2004) that is assured through the efficient cargo movements, commercial relationships and integration among different stakeholders.

An important element of supply chain security is cargo integrity. Cargo integrity is primarily affected by supply chain disruptions (Prokop, 2004), therefore security regulations are being adopted by authorities and agencies so as to standardize the security procedures to minimize the disruptions and improve the overall efficiency. However, the number of different regulations that each organization has to abide with, impact adversely transportation chains in terms of time and costs related to the physical movement of cargo. The stakeholders of the security system can be broadly divided into four categories; customers (Buyer, importer, consignee etc.) suppliers (seller, exporter, consignor) authorities (customs, ports, intervention and border authorities) and intermediaries (freight forwarders, transport companies, brokers, banks, insurance providers etc.). These stakeholders are interested in optimizing their throughput and efficiency without compromising the reliability of the information. Although many supply chain stakeholders are intimidated by the new regulations, nevertheless, they seem to understand that these security initiatives aim to minimize the risk and improve the mitigation effectiveness.

The literature on supply chain security has focused on two major streams of research. The first stream is technical studies that primarily focused on the development of appropriate equipment and/or of advanced forecasting algorithms to detect dubious consignments. For example, Arendt et al., (2012) describe how the project CHINOS is increasing visibility and security by using innovative IT technology like RFID and automatic damage documentation as well as how the project INTEGRITY develops and implements an IT system to increase supply chain visibility. Similarly, the project Contain (CONTAIN Consortium, 2011) develops an innovative container device as well the appropriate IT infrastructure to increase security, whereas the SMART-CM project (SMART-CM Consortium, 2016) was one of the first Research Projects that the European Commission funded to address the improvement of the efficiency of the Authorised Economic Operator (AEO) concept. To this extent, Azaiez and Bier (2007) examined optimal investments in the security of multi-component systems based on the assumption that the defender intends to preserve the overall systemic functionality.

Similarly, some studies focus on developing advanced algorithms to detect suspicious containers or consignments and warn the relevant authorities in advance. Yang et al., (2013) developed an advanced threat-based criticality analysis methodology designed for the identification and prioritization of vulnerable port facilities under uncertainties, combining fuzzy Bayesian reasoning and analytical hierarchy process (AHP) analysis. With respect to game-theoretic studies, a number of researchers

(Sandler and Arce, 2003; Sandler and Lapan, 1988; Basuchoudhary and Razzolini, 2006)) have developed advanced game theoretic models to understand the interactions and the reasoning behind attacking vulnerable assets.

The other stream includes business-oriented studies which explore the value these regulations have on the day to day business up to the strategic level. For example, Rice and Spayd (2005) claim that security upgrades may bring collateral benefits such as trade facilitation, asset visibility following a previous argument set by Sheffi (2001). Willys and Ortiz (2004) argue that supply chain efficiency and security are interrelated in terms of reducing customs delays, increased transparency of information of goods flows, reducing shipping costs among others. In this context, a number of studies have focused on measuring the adverse effects of security regulations on logistics efficiency. Mazeradi and Ekwall (2009) had shown how the implementation of the ISPS-code increases paperwork and slows down processes in ports. Similarly, Stevenson (2005) showed that the ISPS code may have a negative impact on costs and on the efficiency of terminals.

Although the automated systems that are introduced aim at increasing the efficiency and the effectiveness of supply chain processes, there seems to be a gap in the depth of actual integration of these security systems. More precisely, in most of the cases, the information collected or disseminated is either unidirectional or siloed with specific stakeholders. This paper argues in favour of data fusion as a promising alternative to improving the security level in the supply chains, to capitalize on existing equipment and security investment as well as improve the efficiency of security procedures and security red tape through better integration among the different actors[1] of a security system.

Supply chains and information security have been of interest for scholars for decades. Great attention is paid to technical controls to information protection by devising and implementing tools to maintain the flows of high-quality data that ensures the smoothness and safety of information integration among different stakeholders of the supply chain. The information security is designed to minimize the risks arise in the information sharing, which may range from inconvenient (such as loss event happening) to catastrophic (Smith et al., 2007). Information security risk generally refers to the loss or degradation of confidentiality, integrity, or availability of information (Smith et al., 2007; Chellappa and Pavlou 2002; Gordon and Loeb 2002). These risks are minimized through proper information management which according to (Dhillon and Backhouse 2000) has three dimensions; technical (that focus on the automated components of the system such as computers, data networks), formal

[1] Where actors refer to the port users and port service providers (Talley, 2009). The port users include sea- and land-based carriers as well as shippers and passengers. Service providers include port operators such as port authorities, terminal operators or terminal operating shipping lines as well as stevedores, ship agents, pilotage and towage, ship repair and maintenance, customs brokers, freight forwarders, third-party logistics companies, including value-added services and warehousing, governmental and regulatory bodies (Talley, 2009).

(that address the protection mechanisms implemented at the data sharing at the network level including policies, strategies, regulations and standard procedures), and informal (that stresses security at an individual level such as encouraging appropriate attitudes towards information protection and developing shared values and beliefs). In this framework, we have focused on all three aspects. The first two aspects i.e. technical and formal are described in detail whereas the informal aspect (third aspect) is addressed in terms of collaboration between different stakeholders particularly those involved in data sensing stage which is introduced through the use of Radio Frequency Identification (RFID) to encourage participants to share processed data to achieve the target of collaboration and ensure the integration in the information flow (Chow et al., 2007).

2 A conceptual framework to increase container security

2.1 Introduction

A number of studies highlight the growing importance of ports in the maritime trade as ports undertake a significant role in the logistics related activities in the Global transport systems (Notteboom, 2006; Pettit and Beresford, 2009; Beresford et al., 2011; Robinson, 2006). The port is actually a heterogeneous construct of actors, stakeholders, processes and functions (Herz and Flamig, 2014) that need to be integrated to design an effective and efficient container security system. We extend this premise in this study to all terminals since they pose significant nodes in trade flows, especially international.

The concept of an integrated container security approach is based on the premise that key operational processes for logistics management should be efficiently and effectively integrated with container security management processes on the one hand and oversee the secure information flow among different stakeholders on the other hand. We propose a seamless Supply Chain Security Reference Framework (SCSRF) considers a Data Fusion Framework that addresses the container security with respect to different elements that constitute a complex container security network within which the main focus is capturing and processing secure data/information from and to all the relevant stakeholders in the value chain.

According to Bass et al., (2012), a good architecture should be the product of a single architect or a small group of architects with an identified technical leader. Based on this concept the proposed framework has three small groups of architects; supply chain stakeholders, sources of data collection for the system and information flows for data processing which interacts with the technical leader – data fusion network as shown in the following figure.

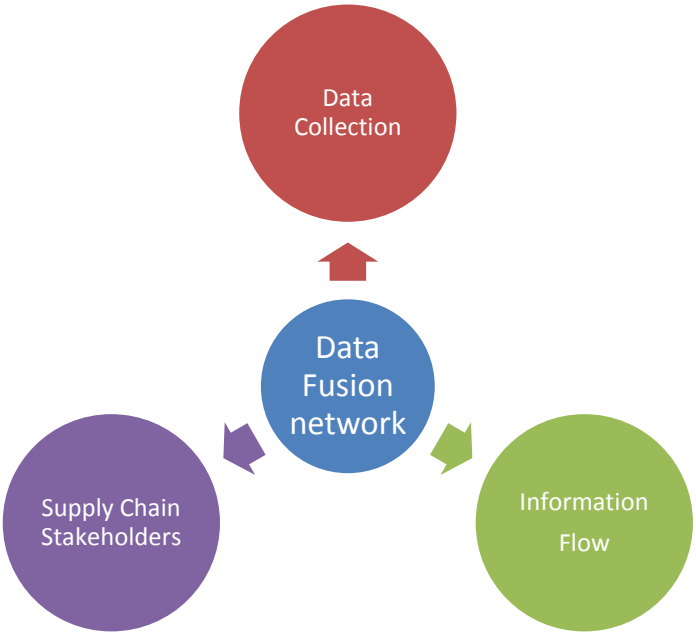

Figure 1 - Conceptual Supply Chain Security Reference Framework

2.2 Supply Chain Stakeholders

2.2.1 Customs and Border Agencies

Customs and border agencies are the major stakeholders of the Supply chain security system who endeavour to improve the estimation process in their risk management approach (Koliousis, 2019) so as to reduce the associated risks. Fusing the above-mentioned information is one of the options customs could use to get advanced alerts and to timely execute robust risk analytics. This gives customs the flexibility to identify specific, pre-flagged, containers and perform more detailed checks and inspections. In order to sufficiently perform this, consignments' information should become available (Morrall et al., 2016) well before the containers arrive in the first port of entry. Entry Summary Declarations (ENS), Single Administrative Documents (SAD) and any such relevant information support consignment-oriented information for risk management rather than simply container-oriented information. The risk analysis is usually based on simple rule-based analytics (relational information, equal to, larger than, less than, not equal to, etc.) that pre-identify suspicious consignments.

2.2.2 Freight and Transport companies

As an important actor and stakeholder in the supply chain security, freight and transport companies aim at optimizing their freight throughput, thus are positively inclined to use live feeds from sensor networks. As a result, information sharing becomes critical not only in terms of operational excellence (Cane et al., 2012) but also from the value chain perspective. This information produces notifications not only about the container content status but also about the container positions, security

features, shrinkage and tampering. That is why this should be a feature-rich and scalable framework which at the same time requires technology and information availability. This information can be complemented by or amended to electronic documentation in order to increase inspection efficiency. This information may also be used to optimize logistical planning and real-time re-planning, especially from a value chain perspective, since it enables real-time transport delay information.

To this extent, freight companies need to fuse planning and status information to all relevant supply chain stakeholders, which should also be extended to relevant value chain stakeholders to increase efficiency. This information is stored in the ERPs/logistics systems, and the electronic messaging is disseminated (Cane et al., 2012) to relevant freight companies, freight brokers, customs, port authorities, container sensor and GNSS/LRIT/AIS information storages to name but a few. Currently, the state of play is sharing raw sensor data (CONTAIN Consortium, 2011), nevertheless, the process upgrade should come from disseminating semantic or semantic-ready content from the sensor reports. Therefore, standardization of the fused data is a primary stakeholder's need which is necessary in order to automate the event, situational pattern and situational awareness recognition. On the value chain level, information fusion and standardization is equally essential since the operator/decision-maker may improve the situational awareness on both the supply and the value chain level on an end-to-end basis, offering a more robust in terms of security assessment of consignments. For example, streaming information compared to suspicious patterns could detect security events for containers (intrusion, movements, tampering, etc.) as well as an earlier warning, decreasing unnecessary and extra costs.

2.2.3 Inter-connectivity among Stakeholders for Supply and Value Chain Resilience

Stakeholders in extended supply and value chains are interested in optimizing their throughput and commercial efficiency. For example, cargo owners are not directly involved in the supply chain operations, however, they benefit from increasing the situational awareness. In order not to open the system to non-relevant stakeholders and retain at the same time the reliability of the information, state-of-play approaches are utilizing Access Point concepts (SUPPORT Consortium, 2010) to perform stakeholder connectivity. We will define Supply Chain Access Point technology as "a system that disseminates predetermined information in the form of standardized short messages on an automated basis to a set of predetermined recipients without delays". Access Points facilitate value chain stakeholders to communicate seamlessly using short messages without passing them through centralized platforms and allow an automated, explicitly pre-defined process. The communication embraces advanced security protocols so as to improve information security.

Access Points benefits arise from their capability to provide singularity in a connected network of applications and to integrate data and dynamically push it to multiple recipients. The interconnectivity among different stakeholders using Data Fusion Framework is shown in the following figure.

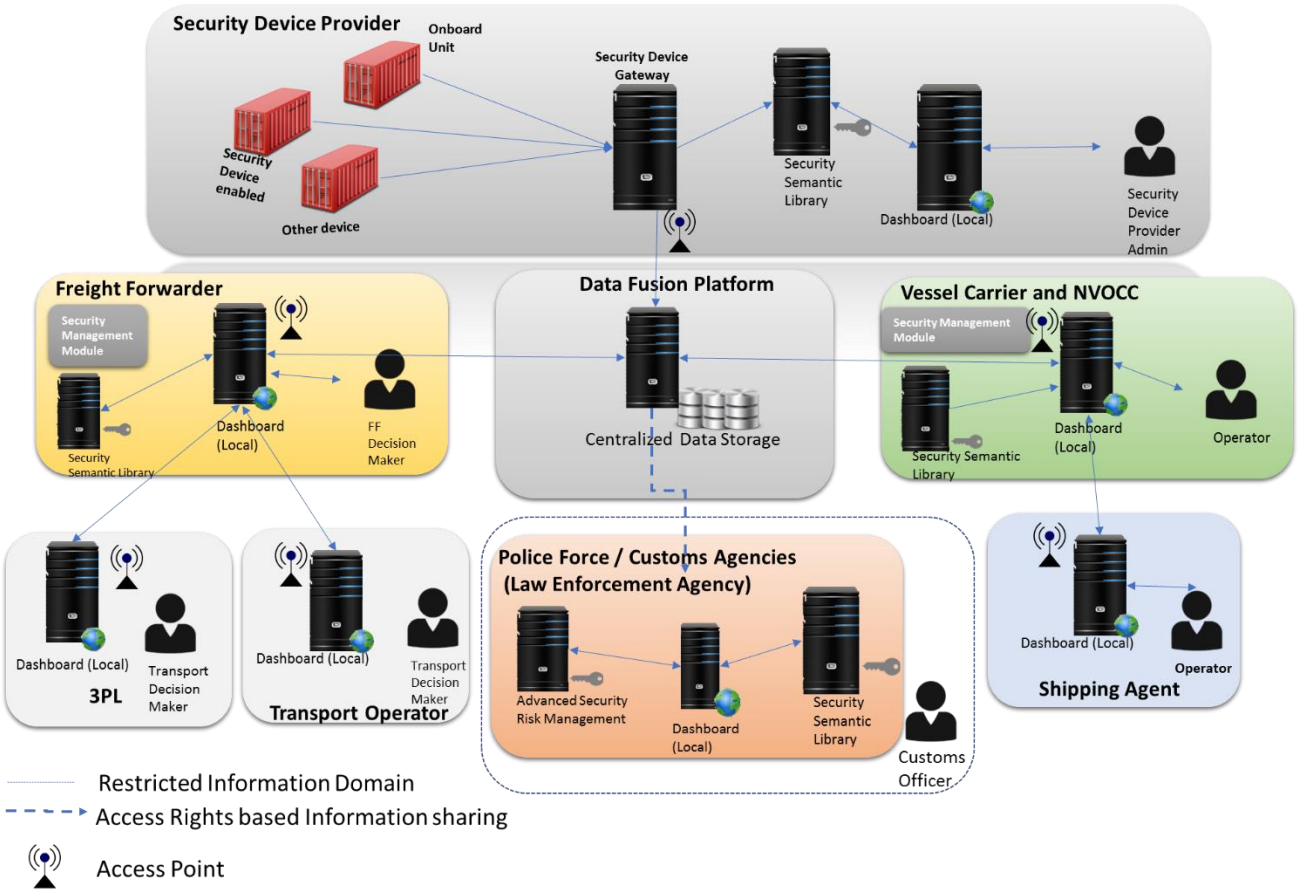

Figure 2 – Collaboration among Supply Chain Stakeholders: exchange of security messages

As per Figure 2, the organizations exchange different security messages and information with the Data Fusion System. This system undertakes a central role in this process by centralizing data collection, however on a pseudo-distributed basis. The Security Device Providers own and operate Supply Chain Security Devices as well as relevant onboard units that collect security-related messages and create alerts. The devices are installed onto vehicles, containers, etc. to monitor the supply chain services. Vessel Carrier and Non-Vessel Operating Common Carriers are global container shipping companies that own and operate or just operate/collaborate fleets of ships and shipping containers. These entities require security alerts to more effectively execute the transport plan, thus they heavily rely on Security Devices Providers to get this information from. They use interfaces for consuming supply chain monitoring data which are pushed into their enterprise applications. Police Forces (including customs authorities) are law enforcement agencies with the responsibility of securing border/ perimeters, carrying out immigration and customs controls, checking illegal activities etc. These authorities have been assigned to operate screening processes, checking documentation, collecting (sensitive) intelligence. Freight forwarders, on the other hand, manage the transfer of cargo thus they also need access to increased security awareness. Transport Operators undertake the movement of cargo and need also advanced security awareness.

It can be easily understood that the proposed framework adopts a centralized approach for security messages. The Data Fusion Platform collects the messages from all related stakeholders and disseminates them to the respective parties. This approach facilitates rule-based or access-based sharing and pushing of information. For example, the data producer's security domain may determine whether a given data consumer has access to the unprotected representation of a particular set of monitoring events. Data consumers may only have access to the unprotected monitoring events if both sub-domains allow them to.

2.3 Data sensing, risk identification, assessment and response in value chains

The main operational objective of custom organisations is to ensure the arriving cargo against legal, fiscal, tax, duty and criminal restrictions. Current risk management practices rely heavily on physical inspections, a practice that produces unnecessary inefficiencies in the entire value chain. Therefore, selecting a number of containers to be inspected, becomes critical in terms of increasing the effectiveness of the risk management system whereas a detailed 100% check is operationally unrealistic. Notably, there are exceptions to this sampling rule; from geographical restrictions like the case of imports to the USA to contextual restrictions like post-incident red level alerts. A number of selection criteria are indicated in different frameworks, like those stipulated in the SAFE Framework (Ireland, 2009). These criteria include country of origin, declared content, weight, value, volume, cross reference of information on Single Administrative Document (SAD) and Entry Summary Declaration (ENS). When the risk assessment is above preset thresholds, the container is isolated for inspection. Although most authorities are using advanced information sources, there is still a long way to go. Additional information that is often unnoticed during the risk estimation includes stakeholder originated information like Bill of Lading information, route selection, route deviation, security history information for the transport company,

ship crew information, truck driver history information, delays, etc. Although elements of this information might be sensitive, commercially or individually, competent authorities may request it and/or is already available on a voluntary basis. For example, the ConTraffic system (Joint Research Center of the European Union, 2017; Varfis et al., 2011) stores and disseminates commercial information to participating authorities in the EU. EU Customs authorities primarily rely on the "Single Administrative Document" and on the "Entry Summary Declaration" as well as on commercial trade databases for the bill of ladings (collected from ports and relevant authorities around the world), including the C-Hawk system. Additionally, there are a number of relevant initiatives from Governmental Agencies like the C-TPAT (CBP, 2016), the AEO (CP3 Group, 2016), (European Commission, 2016) the ISPS Code (International Maritime Organization, 2012) and the SOLAS Convention (International Maritime Organization, 2016). Since this paper focuses on the value chain aspects of security thus will not get into further security-related details of these systems.

The relation between data sensing, risk identification, assessment and response is shown in Figure 3. This relationship diagram highlights a number of features in assessing the information flows where the process begins with Data Sensing from different sources. This information is assessed in order to estimate the Container Risk Index which in turn supports decision making (Risk & Loss assessment) for risk assessment and response. This relationship structure not only supports interactions among business entities but also the information interaction between business entities and governmental bodies and agencies.

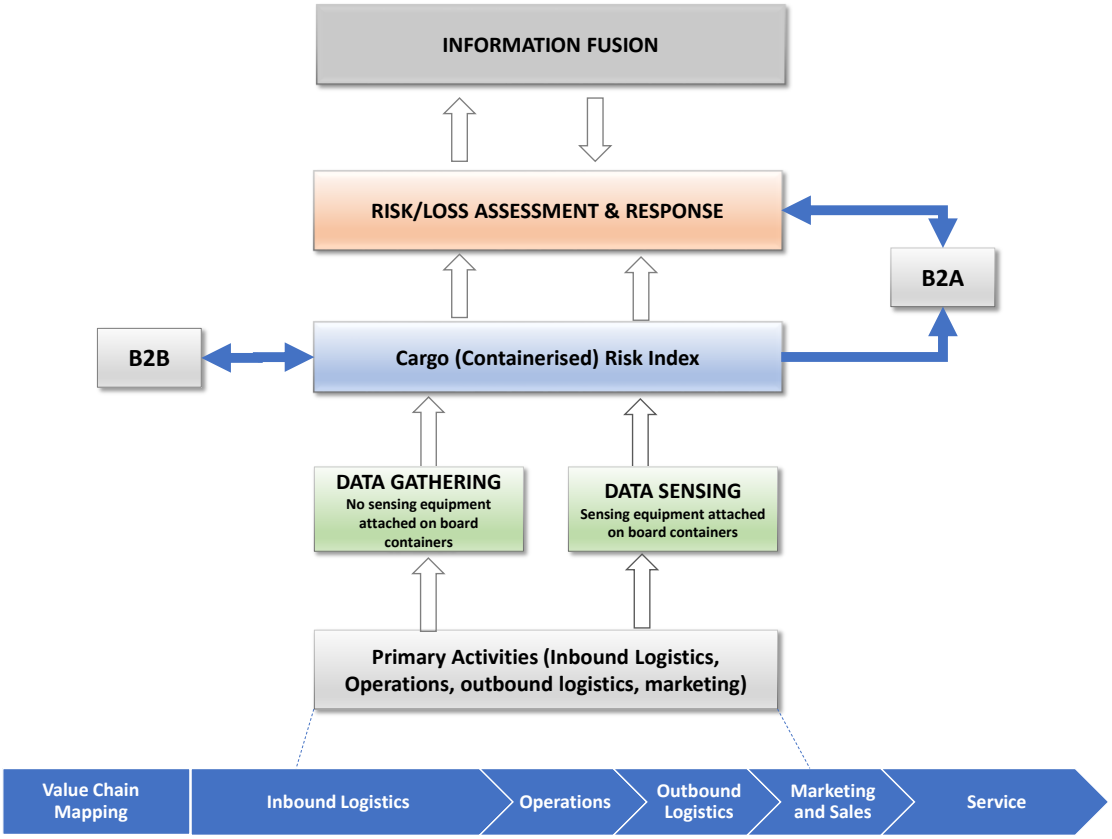

Figure 3 – Data sensing, risk identification, risk assessment and response in a value chain

In this simple relationship framework, the stakeholders from a value chain perspective may use either container with data sensing equipment or containers without data sensing equipment. Data flows contain relevant information that will help both agencies and stakeholders assess the risks and decide on the most appropriate mitigation and response strategies.

2.4 Proposed Data Fusion Framework

As can be easily understood from Figure 3, the seamless and timely exchange of relevant security information is of paramount importance to the success of any security response strategy. In order to facilitate this seamless and timely exchange of messages, we propose a Data Fusion Framework. The architecture (Figure 4) facilitates integration to either network-based, distributed systems or to conventional stand-alone systems and adheres to common data fusion principles, including abstraction, data & task independence, parallel processing, synchronization and modularity.

The framework considers components like sensors, algorithms and fusing procedures as black boxes, an approach that accelerates adoption and makes data flows more seamless. Additionally, each component is independently executable and even parallel with other components whereas the system as a whole is scalable as per the growing requirements. In terms of data needs, independent libraries semantically utilize events (e.g. threats) contextually both with and without data attributes. We will call this Middle-Level Data. This layout facilitates sorting high-level information automatically and in real-time making it extremely practical to constantly monitor specific events.

This framework adopts a quasi-centred fusion and transformation process: on one side, the sensor network providing raw data and alerts to the Data Fusion Platform and on the other side, the Data Fusion Platform itself. With respect to the sensor network, industrial state-of-play has adopted (CONTAIN Consortium, 2011) the Container Security Device – CSD. Once a CSD is activated inside the container, it regularly collects data like temperature, pressure, humidity, light, CBRN attributes of the cargo.

The Rule Engine collects and compares raw data with predefined values contributing to developing an environmental awareness status. Additionally, the Rule Engine includes authentication procedures to verify and validate the content sent therein. This subsystem runs on the backend real-time and supplies information to the workflow engine. Both Business to Business (B2B) and Business to Authorities (B2A) processes entail standardized messages. These messages are then received by the platform users and may be stored locally.

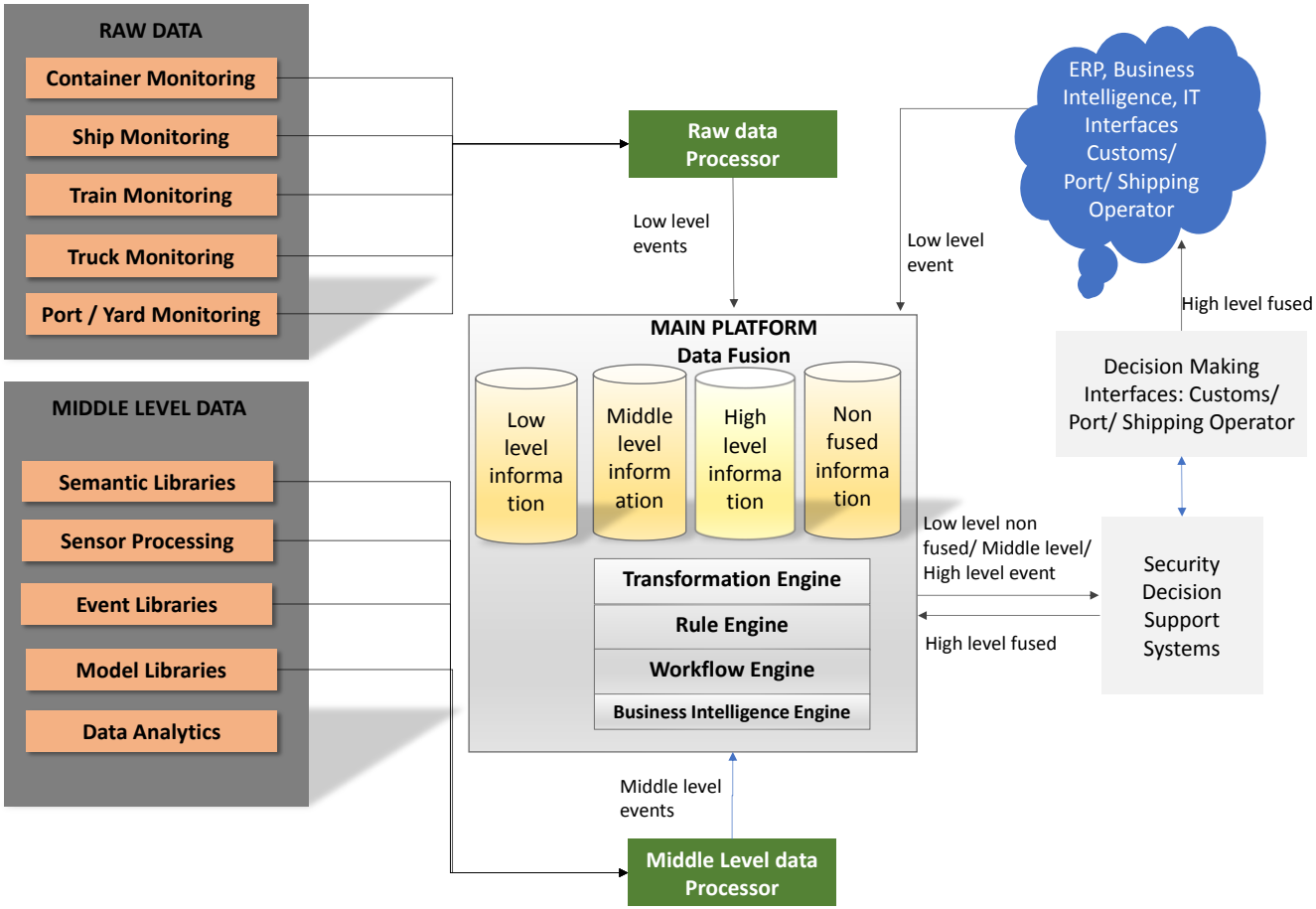

Figure 4 - Data Fusion Framework basic components

2.5 Information Flow and Supply Chain Security – Conceptual Architecture

Supply chains and information security have been of interest for scholars for decades. Great attention is paid to technical controls to information protection by devising and implementing tools to maintain the flows of high-quality data that ensures the smoothness and safety of information integration among different stakeholders of the supply chain. The information security is designed to minimize the risks arise in the information sharing, which may range from inconvenient (such as loss event happening) to catastrophic (Smith et al., 2007). Information security risk generally refers to the loss or degradation of confidentiality, integrity, or availability of information (Smith et al., 2007; Chellappa and Pavlou 2002; Gordon and Loeb 2002). These risks are minimized through proper information management which according to Dhillon and Backhouse (2000) has three dimensions; technical (that focus on the automated components of the system such as computers, data networks), formal (that address the protection mechanisms implemented at the data sharing at the network level including policies, strategies, regulations and standard procedures), and informal (that stresses security at an individual level such as encouraging appropriate attitudes towards information protection and developing shared values and beliefs). In this framework we have focused on all the three aspects. The first two aspects i.e. technical and formal are described in conceptual architecture whereas the informal aspect (third aspect) is addressed in terms of collaboration between different stakeholders particularly those involved in data sensing stage (also described in detail earlier in section 2.2.3) which is introduced through the use of Radio Frequency Identification (RFID) to encourage participants to share processed data to achieve the target of collaboration and ensure the integration in the information flow (Chow et al., 2007).

The fundamental architectural design for a software system emphasize the existence of a number of principles (Chen et al., 2013; Bass et al., 2012) to develop a robust, consistent and scalable system and more precisely, our proposed framework follows these principles:

- ***Modularity:*** this is a critical aspect for developing complex security management systems that consist of different modules interacting in a non-standard manner
- ***Open Standards***: an essential feature to enable more systems to be integrated
- ***Interoperability***: to efficiently and effectively connect distributed and heterogeneous systems
- ***Scalability***: to improve and extend the systems with new processes, workflows, technological advancements
- ***Security***: to balance collaboration among users yet restriction of sensitive information as well as dependability of information,
- ***Privacy***: since commercially sensitive information will be stored and handled on the cloud,
- ***Reusability***: of logic, processes, procedures, workflows so as to easily replicate existing sub-systems to be easily used by Supply Chain agents.

In order to exemplify the information flow and the interactions among the different stakeholders in the conceptual architecture, Figure 5 presents a simple scenario for the collaboration and the message exchange. The proposed Data Fusion Framework supports real-time exchange of directly connected data providers and is the basis of near-real time exchange of cloud connected external data providers. The exchange and collaboration of standard agnostic messages includes primarily GPS, Sensor Alerts, ERP Data, Commercial Data, Security Awareness Data, however this exchange is scalable and extendable. Furthermore, in the case of exchanging higher level messages, for example messages that have been handled to produce semantic information, the proposed system supports different protocols (including HTTP /HTTPS), and methods (including POST, REST, etc) so as to enable more value chain stakeholders engage with.

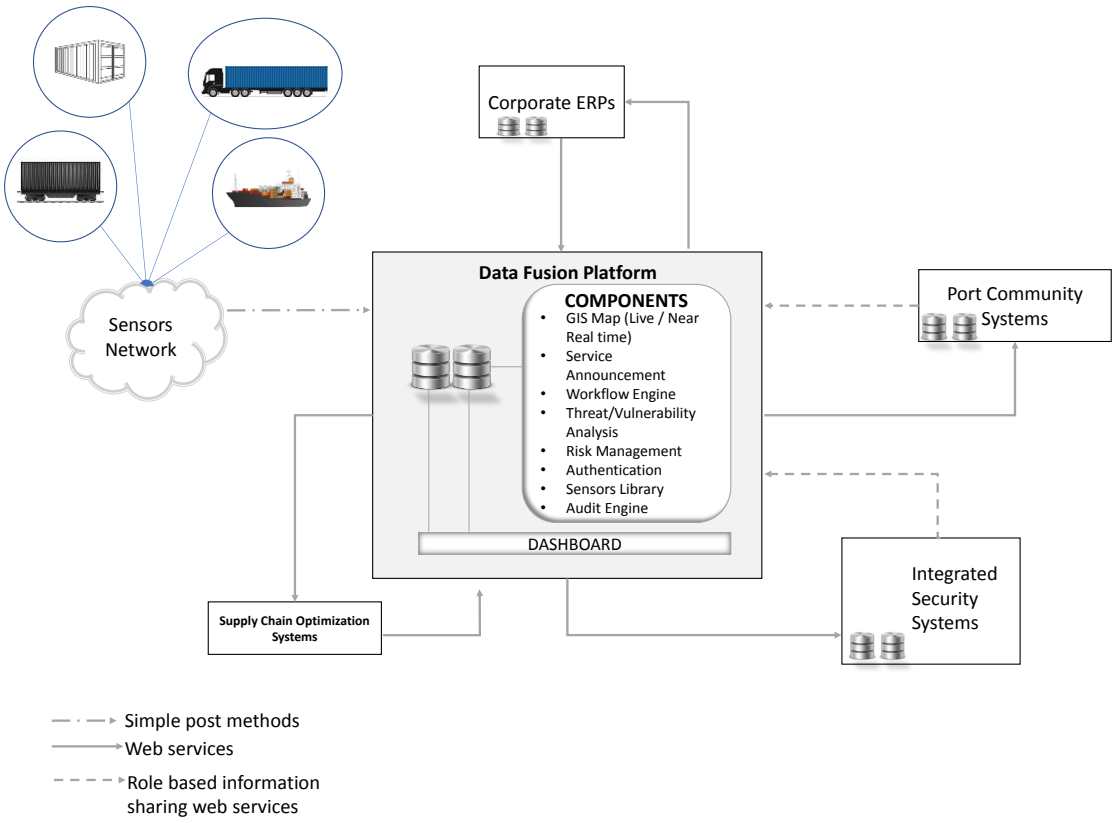

Figure 5 – Information Flows Architectural Design

The framework includes a network of sensors like GPS Devices, RFID, security sensors and onboard units that are configured to regularly send real-time data to the Data Fusion Platform. The platform collects these data as well as any security event and related activity for the entire container transport chain. Subsequently, the system calculates the risk levels and flags them for the user in a semantic approach.

2.6 Case Study: Container Logistics Data & Security Information Exchange

This section explains how the operational attributes of the proposed framework are implemented in the case study. The operational details of the information exchange among the different supply chain stakeholders are identified based on the

OASIS Universal Business Language (UBL) - Intermodal Freight Management process (Universal Business Language Committee, 2013).

In its basic form, the Intermodal Freight Management process (Figure 6) entails three stages. The first stage, ***Planning,*** is where the transport demand is declared in a standardized format, and the Transport Service Providers plan their services accordingly. All support arrangements usually take place in this stage. In procedural terms, Transport Users and Transport Service Providers, develop a Transport Execution Plan which confirms all necessary transport details. With the finalization of the Transport Execution Plan, a Goods Item Itinerary is sent from the Transport Service Provider to the Transport User. The Goods Item Itinerary includes a number of information like the Packing Lists and also provides additional information related to the complete transport service.

The second stage, ***Execution***, contains (a) the physical transport of the cargo and (b) the exchange of supply chain related information. With respect to compliance, the Transport Service Providers exchange regulatory and compliance information with Regulators as well as receive information from Transport Network Managers. The Transport Progress Status message includes all pertinent information.

The last stage, ***Completion,*** confirms delivery and exchange of reports among supply chain stakeholders.

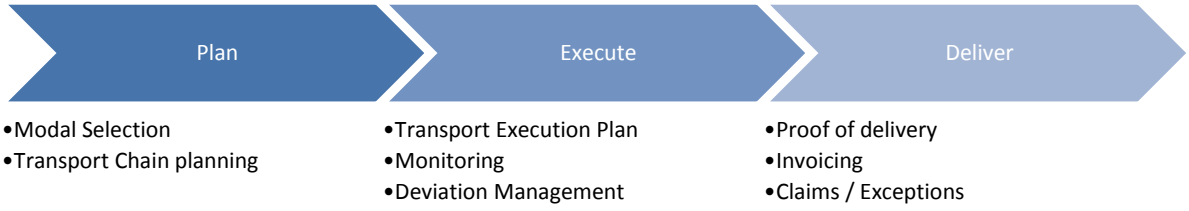

Figure 6 - A Generic Freight Management Process (Universal Business Language Committee, 2013)

These three stages can be further mapped following the UBL conventions (Universal Business Language Committee, 2013) encompassing key Intermodal Freight Management messages including the Transport Service Description, Transport Service Description Request, Transport Execution Plan, Transport Execution Plan Request, Transportation Status, Transportation Status Request, Transport Progress Status, Transport Progress Status Request, Goods Item Itinerary, and Freight Invoice. The Transport Execution Plan message is sent by a transport user to request a transport service from a transport service provider. The Goods Item Itinerary message provides details relating to a transport service, such as transport movement, identification of transport equipment, identification of transported goods, subcontracted service providers, packing lists, etc. The Transportation Status - TS message disseminates reports of the transportation status and/or of event changes. In terms of the structure of the messages, we follow the Common Reporting Schema (CONTAIN Consortium, 2011) providing structure in sharing compliance and regulation related information shared with authorities at any stage of the transportation process.

Table 1 – Message Description

Message Short Name	Message Name	Details
TSD	Transport Service Description	A standardized description of the transport services offered. Standardization enables automatic identification of the services offered.
TEP	Transport Execution Plan	A standardized message that includes information related to the execution of a transport service.
GII	Goods Item Itinerary	A standardized message that includes information about the content of the goods and their movement(s).
TES	Transport Execution Status	Standardized information about the progress of the transport execution.
TOS	Transport Operation Status	Standardized operational information (ETA –Estimated Arrival Time, ETD – Estimated Departure Time, etc).
SDM	Security Data Message	Standardized message providing information about the security of a securitized load unit (e.g. Container, Wagon, etc).
CRS	Common Regulatory Schema	A standardized message which includes compliance-related information for the authorities.
TNS	Transportation Network Status	A standardized message announcing the state that a network or part thereof currently is.
CRP	Container Risk Profiling	A standardized description of the risk reporting of each container, based on the consignments it carries.
CIO	Container Review Order	A standardized order to relevant regulatory authorities to stop a load unit and further examine it.

Source: Adapted from (CONTAIN Consortium, 2011)

In order to explain in more detail the messages that the different supply chain stakeholders exchange, an actual operational case is presented in Figure 7. This is a simple case, where the supply chain stakeholders interact with one another sharing messages and making decisions based on this information. More precisely, the Logistics Service Provider pushes different messages to the relevant stakeholders and to the Data Fusion Platform. The objective is to report effectively and sufficiently different states as well as different relevant transport information the earliest possible. A trigger point is then appearing in this process and initiates a decision point where the transport chain providers (part of the value chain stakeholders) choose to amend the Transport Execution Plan if this is considered necessary.

For example, one task is the monitoring of the condition of the cargo, which may be the trigger event that informs the Transport Execution Status message. This task includes the collection, the registration and the control of environmental conditions data like the temperature, the humidity, the pressure, the light / infrared light, the acoustic and the pressure inside by the CSD and the sending of the message to the Data Fusion Platform. When the CSD is activated after a cargo condition event triggers it, the platform starts collecting this data in order to inform and adapt the Transport Execution Plan. From a value chain perspective, this informs the different stakeholders to adapt their activities and their operational actions. Depending on the developed solution, alarms are generated and transmitted on either a centralized or a distributed basis through the Data Fusion Platform. An information security structure ensures that only authenticated stakeholders can send and receive information, whereas validation is executed both centrally and locally (in the distributed manner).

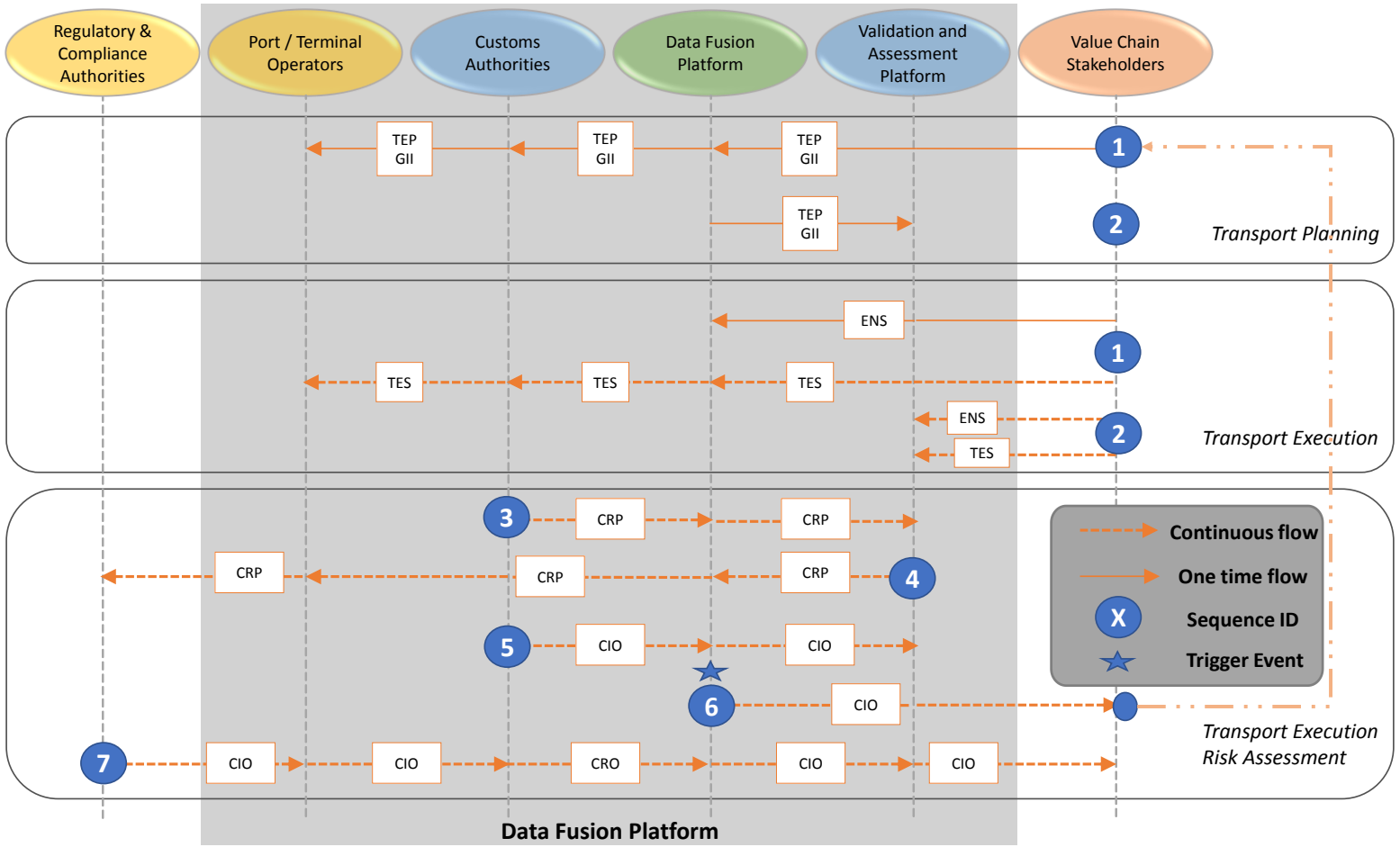

Figure 7 - Information flow among supply chain stakeholders (adapted from (CONTAIN Consortium, 2011))

3 Conclusions

The introduction of security monitoring and inspection processes are a reality in modern supply chains. Considering this reality, this paper has addressed how we can improve the supply chain efficiency with the presence of such security initiatives. Security-related data is needed on a real-time basis and a system that can adequately support this will support security procedures more effectively. Keeping this in view, this research proposes a simple framework that facilitates improved security for data sharing among supply chain stakeholders by providing rule/principles based access to security information in real-time that enables not only the optimization of the supply chain but more importantly improves the data security level.

The proposed conceptual framework is expected to improve overall value in the supply chain through the innovative data fusion network that will:

- improve supply chain planning upstream and downstream;
- reduce administrative red tape;
- improve security levels;
- improve supply chain integration through the improved monitoring of the cargo integrity;
- increase flexibility to cope with increasing trade volumes;
- increase trader trust throughout the value chain;
- improve transaction and turnaround times in ports, terminals, inland terminals;
- reduce administrative compliance activities and processes
- decreased fraud
- to improve collaboration and interoperability with other border agencies and enforcement organizations.

4 Policy & Research Recommendations

Developing mechanisms to effectively share information among different stakeholders of the security system is a domain with high value therefore, future research should provide more empirical data to assess the value of different security mechanisms in the supply chains. Additionally, there is need to undertake more research on the reengineering of the processes to minimize the impacts of security incidents because this is one of the greatest challenges in supply chain security. This paper proposes a simple solution to a complex reality however, more advanced data fusion frameworks should be explored.

With respect to policy implications of the research, this framework requires a top-down approach so as to be further exploited. The security domain is heavily regulated and as such, centrally imposed decisions enable better usage of such frameworks. Nevertheless, the main tradeoff that has to be decided is whether the sharing of security information may reduce the value and additionally which rules may be adopted to retain this value. In any case, experience has shown (as expressed in the

case study) that spreading information to trusted parties, improves the overall security level.

5 Glossary

AEO	Authorized Economic Operator
CBRN	Chemical, Biological, Radiological and Nuclear
CSD	Container Security Device
EFTA	European Free Trade Association
ENS	Entry Summary Declaration
GNSS	Global Navigation Satellite System
ICS	Import Control System
ICT	Information and Communication Technology
IIP	Integrated Information Platform
ISPS Code	International Ship and Port Security Code
LRIT	Long-Range Identification and Tracking
RFID	Radio Frequency IDentification
SAD	Single Administrative Document
SCSF	Supply Chain Security Framework

6 Disclaimer

Part of this work is based on the CONTAIN Project which was funded by the European Commission under the FP7/SEC/2010/1/261679 Contract.

7 Bibliography

1) Arendt, F., Meyer-Larsen, N., and Mueller, R. (2012). Practical approaches towards enhanced security and visibility in international intermodal container supply chains. Int. J. Shipping and Transport Logistics, 4(2), pp. 182-196.
2) Azaiez, M., & Bier, V. (2007). Optimal resource allocation for security in reliability systems. European Journal of Operational Research, pp. 773-786.
3) Balmata, J.-F., Lafonta, F., Maifretb, R., & Pessel, N. (2009, November). MAritime RISk Assessment (MARISA), a fuzzy approach to define an individual ship risk factor. Ocean Engineering, pp. 1278–1286.
4) Bass, L., Clements, P., and Kazman, R. (2012). Software Architecture in Practice. Addison - Wesley.
5) Basuchoudhary, A., and Razzolini, L. (2006). Hiding in plain sight - using signlas to detect terrorists. Public Choice, pp. 245-255.
6) Beresford, A., S.-H. Woo, and S. Pettit. (2011). “Improving Port Performance: From Serving Ships to Adding Value in Supply Chains.” In Integrating Seaports and Trade Corridors, edited by P. Hall, R. J. McCalla, C. Comtois, and B. Slack, 137–154. Farnham: Ashgate.

7) Cane, T., Mattheis, S., Tsoukos, G., Focas, C., & Koliousis, I. (2012). The e-Freight Multimodal e-Waybill. e-Freight conference. Munich.
8) CBP. (2016). C-TPAT: Customs Trade Partnership Against Terrorism. Retrieved from C-TPAT: Customs Trade Partnership Against Terrorism: http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat
9) Chellappa, R.K. and Pavlou, P. A., (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management, 15, pp.358–368.
10) Chen, L., Ali-Babar, M., & Nuseibeh, B. (2013). Characterizing Architecturally Significant Requirements. IEEE Software, 30(2), 38-45.
11) Chow, H.K.H., Choy K.L., Lee, W.B., Chan, F.T.S. (2007). Integration of web-based and RFID technology in visualizing logistics operations – a case study. Supply Chain Management: An International Journal, 12(3), pp.221–234.
12) Closs, D.J. and McGarrell, E.F. (2004), "Enhancing security throughout the supply chain", IBM Center for the Business of Government, Washington, DC.
13) CONTAIN Consortium. (2011). Container Security Advanced Information Networking.
14) CP3 Group. (2016). AEO Guidelines. Retrieved from AEO Guidelines: http://www.cp3group.com/attachments/AEO%20guidelines.pdf
15) CYSM Consortium. (2013). Collaborative Cyber/Physical Security Management System (Grant Agreement No 4000003750 (Co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union).
16) Dhillon, G. & Backhouse, J., (2000). Information System Security Management in the New Millennium. Communications of the ACM, 43(7), pp.125–128.
17) ENISA. (2011). First annual report of cyber incidents in the EU: 51 severe outages reported over 2011.
18) Ernst and Young. (2012). Global Information Security Survey: Fighting to close the Gap.
19) European Commission. (2003). COMMISSION REGULATION (EC) No 2286/2003. Brussels: European Parliament. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:343:0001:0123:en:PDF
20) European Commission. (2003). Commission Regulation (EC) No 2286/2003 of 18 December 2003 amending Regulation (EEC) No 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No 2913/92 establishing the Community Customs Code. Btussels: European Parliament. Retrieved from http://ec.europa.eu/taxation_customs/customs/procedural_aspects/general/sad/index_en.htm
21) European Commission. (2006). Commission Recommendation establishing a common "Practical Handbook for Border Guards (Schengen Handbook)".
22) EUROPEAN COMMISSION. (2010). A Digital Agenda for Europe COM(2010) 245 final/2 .
23) European Commission. (2016). Authorized Economic Operators – Guidelines. Retrieved from Authorized Economic Operators – Guidelines:

https://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_sec
24) European Commission. (2017). European Customs Information Portal. Retrieved from http://ec.europa.eu/ecip/help/faq/ens7_en.htm
25) European Port Community Systems Association. (2012). Port Community Systems. Retrieved from http://www.epcsa.eu/port-community-systems
26) FRONTEX. (2012). Best Practice Technical Guidelines for Automated Border Control Systems.
27) Future Travel Experience. (2011). Taiwan trials automated border control. Retrieved from http://www.futuretravelexperience.com/2011/03/taiwan-trials-automated-border-control.
28) Gordon, L. A. and Loeb, M.P., (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), pp.438–457.
29) Herz, N.; Flamig, H. (2012). Integrating supply chain management strategies in port logistics: defining requirements for port actors, in Proceedings of 9th International Meetings on Logistics Research. 15–17 August 2012, Montreal, Canada. Association Internationale de Recherche en Logistique.
30) International Maritime Organization. (2002). IMO adopts comprehensive maritime security measures. Retrieved from http://www.imo.org/blast/mainframe.asp?topic_id=583&doc_id=2689
31) International Maritime Organization. (2010). ISM Code and Guidelines on Implementation of the ISM Code 2010.
32) International Maritime Organization. (2012). GUIDE TO MARITIME SECURITY AND THE ISPS CODE.
33) International Maritime Organization. (2016). International Convention for the Safety of Life at Sea (SOLAS), 1974. Retrieved from International Convention for the Safety of Life at Sea (SOLAS), 1974: http://www.imo.org/en/About/conventions/listofconventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx
34) International Standardization Organization. (2005). ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management.
35) International Standardization Organization. (2008). ISO 9001:2008: Quality management systems -- Requirements.
36) International Standardization Organization. (2009). ISO 9004:2009: Managing for the sustained success of an organization - A quality management approach.
37) International Standardization Organization. (2009). ISO/DIS 31000: Risk management — Principles and guidelines on implementation.
38) Ireland, R. (2009). The WCO SAFE Framework of standards: Avoiding excess in global supply chain security policy. World Customs Organization.
39) JRC - Joint Research Center of the European Union. (2017, 08 10). ConTraffic Online Services. Retrieved from https://contraffic.jrc.ec.europa.eu/
40) Koliousis, I. (2019). A conceptual framework that monitors port facility access through integrated Port Community Systems and improves port & terminal

security performance. International Journal of Shipping and Transport Logistics, forthcoming.
41) Mazeradi, A., & Ekwall, D. (2009). Impacts of the ISPS code on port activities – a case study on Swedish ports. World Review of Intermodal Transportation Research, 2(4), pp. 326-342.
42) Morrall, A., Rainbird, J., Katsoulakas, T., Koliousis, I., & Varelas, T. (2016). e-Maritime for Automating Legacy Shipping Practices. Transportation Research Procedia, 143-152. doi:https://doi.org/10.1016/j.trpro.2016.05.050
43) Murphy, P.R. and Wood, D.F. (2008), Contemporary Logistics, 9th ed., Pearson Education, Upper Saddle River, NJ.
44) Notteboom, T. (2006). Fostering seaports – and beyond: challenging the challengers, in Proceedings of ITMMA Maritime and Port Symposium. 25–28 October, 2006, Antwerp, Belgium. Institute of Transport and Maritime Management.
45) Pettit, S. J., and A. K. C. Beresford. (2009). "Port Development: From Gateways to Logistics Hubs." Maritime Policy & Management 36 (3): 253–267.
46) Port of Helsinki . (n.d.). Port of Helsinki West Terminal. Retrieved from http://www.portofhelsinki.fi/passengers/west_terminal
47) PriceWaterhouse Coopers. (2013). The Global State of Information Security Survey 2013.
48) Prokop, D. (2004). Smart and safe borders: the logistics of inbound cargo security. International Journal of Logistics Management, 15(2), 65-75.
49) Rice, J., & Spayd, P. (2005). Investing in Supply Chain Security: Collateral Benefits. Washington DC: IBM Center for Business of Government.
50) Robinson, R. (2006). "Port-Oriented Landside Logistics in Australian Ports: A Strategic Framework." Maritime Economics & Logistics 8 (1): 40–59.
51) Sandler, T., & Arce, D. (2003). Terrorism & Game Theory. Simulation & Gaming, p. 3190337.
52) Sandler, T., & Lapan, H. (1988). The calculus of dissent: an analysis of terrorists' choice of targets. Synthese, pp. 245-261.
53) Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. International Journal of Logistics Management, 12(2), pp. 1-11.
54) SMART-CM Consortium. (2016). SMART Container Chain Management. Retrieved from SMART Container Chain Management: http://www.smart-cm.eu/
55) Smith, G.E., Watson, K.A., Baker, W.H. and Pokorski, J.H. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. International Journal of Production Research, 45(11), pp.2595–2613.
56) Stevenson, D. (2005). The impact of ISPS code on seafarers. International Conference Security of Ships, Ports & Coasts. Halifax, Nova Scotia.
57) SUPPORT Consortium. (2010). SUPPORT - Security UPgrade for PORTs.
58) Talley, W. K. (2009). Port Economics. Abingdon: Routledge. 232 p.
59) The World Bank. (2011). Border Management Modernization.
60) United Nations. (2003). The Single Window Concept.

61) Universal Business Language Committee. (2013). Universal Business Language Version 2.1. Retrieved from http://docs.oasis-open.org/ubl/prd3-UBL-2.1/UBL-2.1.html
62) US Coast Guard. (2010). Maritime Security Risk Analysis Model: Overview for USCG-CREATE Maritime .
63) Varfis, A., Kotsakis, E., Tsois, A., Donati, A., Sjachyn, M., Camossi, E., Pellissie, m. (2011). ConTraffic:Maritime container traffic anomaly detection. International Workshop on Maritime Anomaly Detection. Tilburg: Tilburg University.
64) Willys, H., & Ortiz, D. (2004). Evaluating the Security of the Global Containerized Supply Chains. Santa Monica CA: RAND Corporation.
65) Yang, Z., Ng, A., & Wang, J. (2013). Prioritising security vulnerabilities in ports. Int. J. Shipping and Transport Logistics, 5(6), pp. 622-636.